「フィッシング、クレジットカード不正の現状と対策を考える会」
開催報告

セーファーインターネット協会（会長：中山　明　以下、SIA）は、2022 年 9 月 1 日に、警察庁、経済産業省、かっこ株式会社、ヤフー株式会社、PayPay 株式会社、株式会社メルカリと共同で EC 事業者やクレジットカード事業者、その他の関連団体と、報道関係者の皆さまを対象に「フィッシング、クレジットカード不正の現状と対策を考える会」を開催しましたのでご報告します。

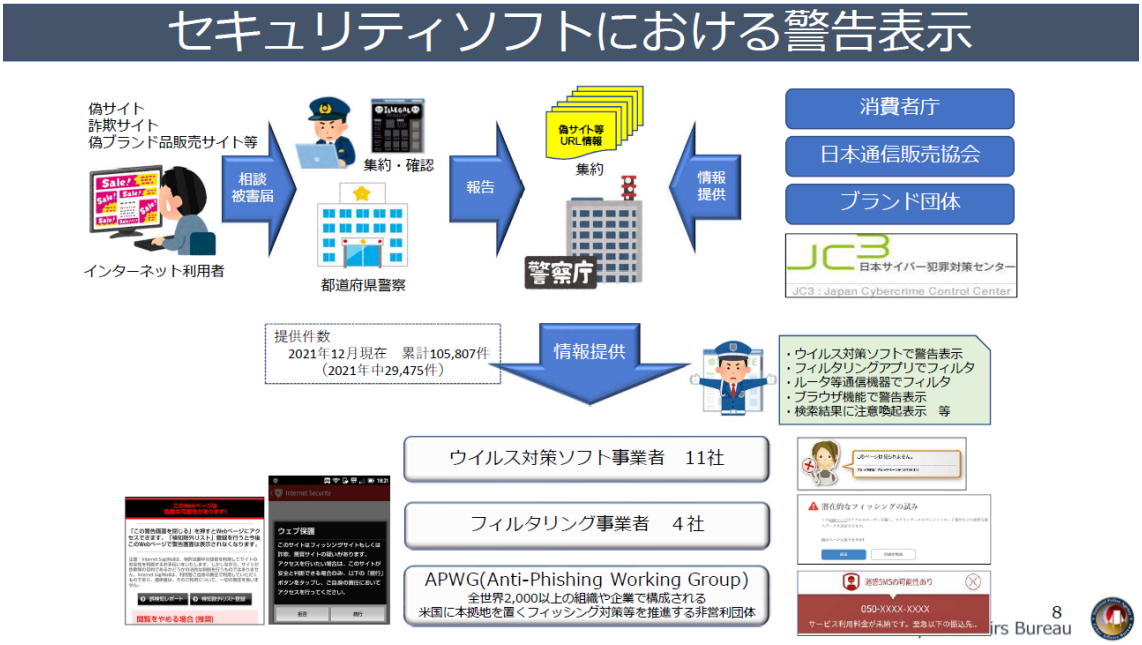
日本クレジット協会によると、2021 年における全国のクレジットカード不正利用被害額は 311 億円と過去最高を記録しており、フィッシングに関しても 2021 年の発生件数は 526,504 件と 2020 年比で約 2.3 倍にものぼります。様々なフィッシングや不正決済の被害が広がる中、EC 事業者、決済事業者においても、お客様への注意喚起や独自のセキュリティ施策など、対策を強化して一方で、フィッシングサイトや犯行の手口が多様化・巧妙化しており、個社での対策に加え、EC 事業者・決済事業者・関係する業界団体といった EC 業界全体で連携を強化し、セキュリティ対策に取り組んでいくことが必要不可欠です。

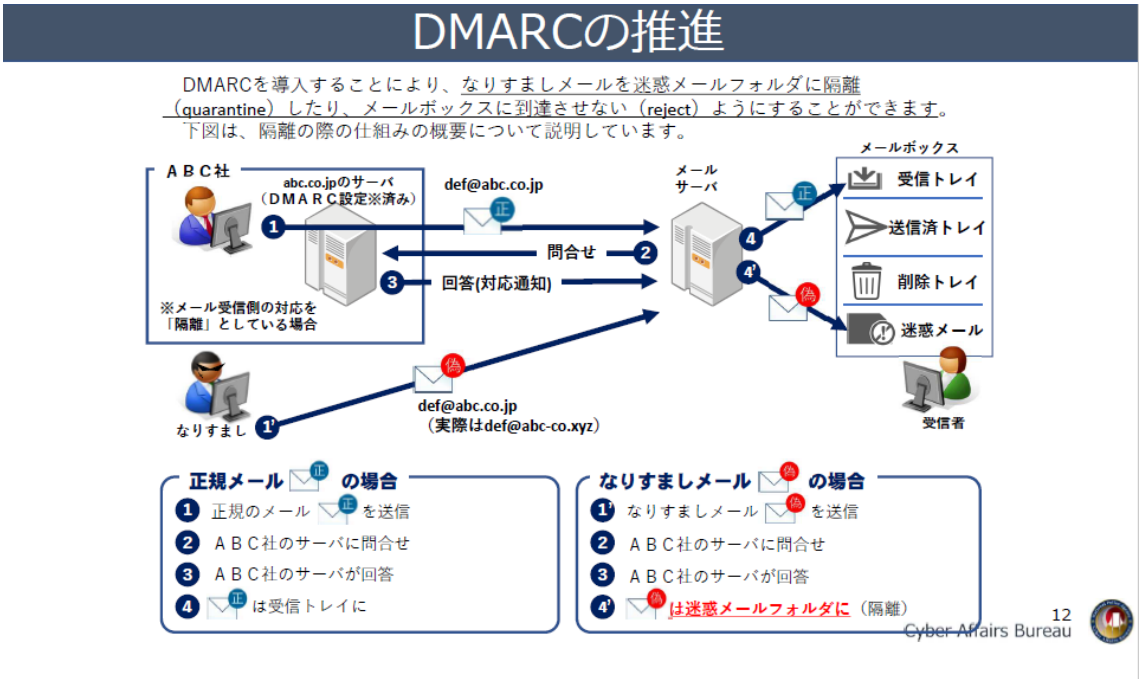
このような背景をうけ、今回は、事業者、関連団体および報道関係者の皆さまを対象に、フィッシング・不正決済の背景と実態、防止対策に関する理解を深めていただくことを目的として開催しました。

基調講演：警察庁　サイバー警察局サイバー企画課課長補佐　清川敏幸氏

警察庁からは、クレジットカード不正利用の手口と警察庁におけるフィッシング対策についてお話をいただきました。

「警察庁が把握しているクレジットカード不正利用の特徴的な手口としては 2 つある。1 つ目はダークウェブから他人のクレジットカード情報を購入した A が不正利用者 B に転売する。B はクレジットカード情報を使い EC サイトで商品を購入して特定の場所へ発送するパターン。2 つ目はフィッシングサイトを作成し、不正に取得したクレジットカード情報を自分のアプリに紐づけて商品を不正に購入するパターンである。
警察庁が行っているフィッシングサイト対策として、都道府県警察からフィッシングサイトの情報を受け、ウイルス対策ソフト事業者に情報提供を行っており、セキュリティソフトを入れているユーザーが該当するサイトを見たときに、警告表示がなされる仕組みです」とのこと。





また、清川氏から、メールを送信する事業者が導入することでなりすますしメールが届かなくなる送信ドメイン認証技術である『DMARC』の紹介があり、「警察庁としては事業者に DMARC の導入を働きかけている」と導入を呼びかけました。

基調講演：経済産業省　商務・サービスグループ　商取引監督課　セキュリティ専門官　小西　啓介氏

経済産業省からは、「クレジットカード決済のセキュリティ対策強化に向けた経済産業省の取り組みなど」についてお話をいただきました。

「経済産業省はクレジットカードの不正対策に長年にわたり対策を行っている。クレジットカード関連の規制をする法令には割賦販売法があり、①クレジットカード番号の適切な管理、②不正利用の防止の義務、③加盟店の調査等の義務、④不正な手段によるカード番号の取得禁止がある。

令和2年の改正では、従来、規制の対象となる事業者は、カード会社と加盟店に加えて、対象範囲を拡大し、決済代行事業者、QR コード事業者、EC モール事業者も対象となる。これらの対象事業者に対してはセキュリティ対策として『PCI DSS』の準拠を求めている。この PCI DSS は 2022 年 3 月に version4.0 へのバージョンアップが行われ、オンラインスキミングやフィッシングなどの攻撃手法への対応が規程された。

また割賦販売法での規程ではなく、クレジットカード・セキュリティガイドラインを策定し、EMV-3D セキュアの導入が推奨されている。

②法令等：割賦販売法の令和２年改正について

- **決済代行業者の役割の増大や、新たな後払い決済サービス提供主体の登場により、クレジットカード番号の情報漏えいリスク**に対する懸念が高まっていることを踏まえ、「割賦販売法の一部を改正する法律」を令和３年４月１日に施行し、**クレジットカード番号等の適切管理の義務主体の拡充**を行った。

クレジットカード番号等の適切管理の義務主体の拡充

クレジットカード番号等取扱事業者	主な対象事業者	セキュリティ対策	違反に対する措置等
1号 ・・・ イシュアー 「クレジットカード等購入あっせん業者」（二月払含む）	・クレジットカード会社等	PCI DSS準拠 同等以上	改善命令・罰金 報告徴収・立入検査等
2号 ・・・ 加盟店 （旧法３号） 「クレジットカード等購入あっせん関係販売業者」 「クレジットカード等購入あっせん関係役務提供事業者」		非保持 または、PCI DSS準拠	報告徴収・立入検査
3号 ・・・ アクワイアラー （旧法２号） 「立替払取次業者」	・クレジットカード会社等	PCI DSS準拠 同等以上	改善命令・罰金 報告徴収・立入検査等
4号 ・・・ 決済代行業者 「立替払取次業者（３号）のために、加盟店に対して、立替金の交付を行う事業者」	・**決済代行業者**（ネット取引、対面取引双方） ・**EC モール事業者** 等	PCI DSS準拠 同等以上 ※対面は、非保持可	改善命令・罰金 報告徴収・立入検査
5号 ・・・ 利用者向け決済サービス 「利用者から提供を受けたクレジットカード番号等を用いて、次回以降、当該クレジットカード番号等を入力することなく、商品購入等を行うことができるサービスを提供する事業者」	・QR コード決済事業者 ・スマートフォン決済事業者 ・ID 決済事業者等 その他名称の如何にかかわらず、クレジットカード情報と紐づけた他の決済用番号で決済を行う事業者	PCI DSS準拠 同等以上	改善命令・罰金 報告徴収・立入検査
6号 ・・・ 利用者向け決済サービス委託先 「第５号の事業者が提供する決済サービスについてクレジットカード番号等の管理を受託する事業者」	・第5号事業者からクレジットカード情報の管理を受託している事業者 等	PCI DSS準拠 同等以上	改善命令・罰金 報告徴収・立入検査
7号 ・・・ 加盟店向け決済システム提供事業者 「後払い決済において、立替払取次業者にクレジットカード番号等を提供する事業者」（２号に対し提供）	・決済代行業者（ネット取引、リアル取引双方） ・**EC システム提供会社** 等 ASP/SaaS として EC 事業者にサービス提供する事業者、EC 事業者に購入プラットフォームを提供する事業者	PCI DSS準拠 同等以上	改善命令・罰金 報告徴収・立入検査

追加

今後のセキュリティ対策の方向性には３つの柱があり、1 つ目は漏洩防止の対策として、さらなる制度的措置の必要性の検討や脆弱性対策の強化。2 つ目は不正利用の対策として EMV 3-D セキュアといった取引認証の原則化や事業者間の共同システム構築、リアルタイム通知の普及などを進める点、3 つ目はフィッシング防止の対策として送信ドメイン認証である DMARC の導入を求める」とお話をいただきました。

③クレジットカード番号セキュリティ対策の３つの方向性

クレジットカード会社等　加盟店　利用者　PSP等

目的意識	これまでの取組	今後の方向性
クレジットカード番号を安全に管理する（漏えい防止）		
▌クレジット決済に関与するプレイヤーは、クレジットカード番号を取り扱う上でシステム等の安全性を確保する	✓ 割賦販売法に基づく対応 （クレジットカード番号等の適切管理規定） － PCI DSS準拠相当 － 非保持化	✓ **さらなる制度的措置の検討** －クレジットカード・セキュリティガイドラインでのアップデート ✓ 加盟店やPSP等のECサイト、システムの**脆弱性対策の強化**
クレジットカード番号を不正利用させない（不正利用防止）		
▌決済を承認する際には認証を行い、なりすましをさせない	✓ 割賦販売法に基づく対応 － 対面取引におけるIC決済の推進 － 非対面取引における本人認証の導入 （セキュリティコード・静的パスワード等における認証）	✓ 特に非対面取引における**取引認証の原則化** ✓ **取引認証方法の高度化** 生体認証・ワンタイムパスワード等といった強力な認証方法を推進 ⇒**EMV-3Dセキュアの普及**
▌決済取引をモニタリングし、不正利用を検知する	✓ クレジットカード会社等における個社での不正検知の取組 ✓ 明細、利用履歴の確認（クレジットカード会社等における明細通知・利用者における確認）	✓ 共同システムの構築・新しい技術や方法に基づく不正利用検知のイノベーション ✓ 明細による確認強化（**リアルタイム通知**等、利用者へのアラート機能の充実）
クレジットの安全・安心な利用に関する周知・犯罪の抑止（フィッシング防止等）		
▌利用者は、悪意を持った第三者からのフィッシング被害に遭わないよう対策を行う	✓ フィッシング対策協議会や日本クレジット協会等における周知啓発	✓ フィッシング対策に向けた多層的な取組（**送信ドメイン認証（DMARC）**等） ✓ 周知啓発の強化 ✓ 事業者と行政機関等における連携強化
▌漏えい防止・不正利用防止で行き届かない部分については、執行で対応	✓ 割賦販売法第49条の２（クレジットカード番号の不正利用・取得）／不正アクセス禁止法等に基づく執行対応	✓ 経済産業省と警察庁（サイバー警察局等）との連携強化

かっこ株式会社　O-PLUX 事業部 ディビジョンマネジャー　小野瀬まい氏

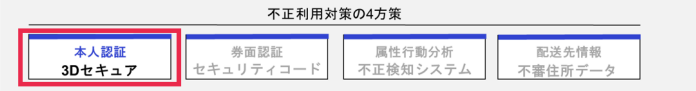
かっこ株式会社からは「EC 事業者における不正被害の実態や対策状況について」お話をいただきました。

「EC サイトにおけるクレジットカード不正利用は 2021 年過去最高となったが、増加の背景には、3 つの要因がある。1 つめは個人情報の売買で、漏洩事故やフィッシングなどで流出したカード情報が、ダークウェブ上で売買されている点、2 つ目は、EC サイトではクレジットカード番号と有効期限のみで決済できるため、被害が発生している点。3 つ目は、購入した商品が転売できるという現金化の多様化である。

また情報漏えいも増加傾向にあり、EC サイトではカード情報を持たない『非保持化』が進んだものの、不正アクセスやペイメントモジュールの改ざん、フィッシングメール通知など、さまざまな手口で情報漏えいが発生している。

かっこ株式会社では 2021 年 12 月に、EC 事業者に実態調査を実施し 546 件の回答があった。クレジットカード不正対策義務化を 7 割が認識していながら、被害負担が EC 事業者であることを 3 人に 1 人は知らない、という現状が明らかとなった。また約 40%の事業者で不正対策に取り組めおらず、その理由としては『被害額が少ない』『優先順位が低い』という理由であった。

不正対策方法：EC事業者の声「EMV3Dセキュア」について



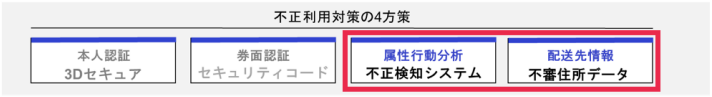
①リスクの高い取引のみ認証になるので、カゴ落ち低減を期待できる
②パスワードが漏えいしても突破されないので安心
③決済が伴わなくてもEMV3Dセキュアの利用が可能
④アプリでも対応可能

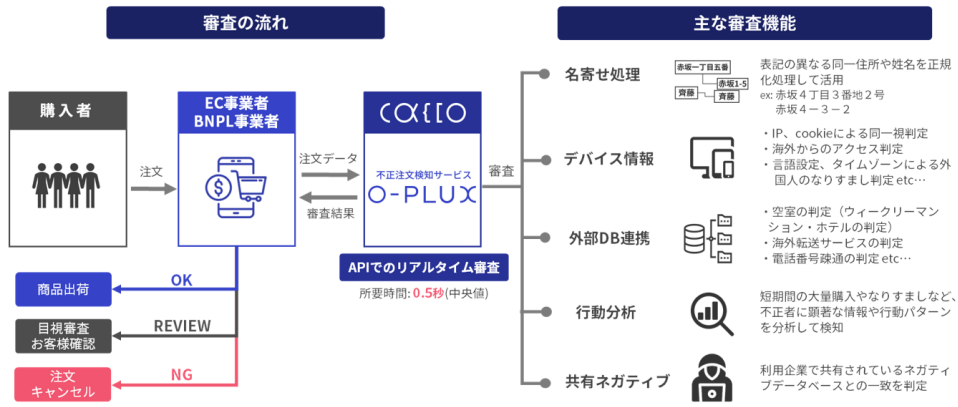
①システム開発コストが数百万円かかる
②EMV3Dセキュアにはランニング費用がかかる
③リスクベース認証の基準は自社の商材や客単価にあってるのか不安
④ワンタイムパスワードが突破される事例も出てきており、すり抜けが心配

不正利用対策で注目される、EMV 3-D セキュアについて、EC 事業者から寄せられる声の紹介もありました。カゴ落ち低減への期待や、パスワードが漏洩しても突破されないという安心感があるという声があるが、他方で、システム開発費やランニングコストがかさむ、といった懸念も多く寄せられている。

かっこ株式会社の不正注文検知サービス『O-PLUX』では、様々なデータを利用して不正を検知するサービスで、サービスを利用されている 2 万サイトのネガティブ情報を共有することで対策することができる。」

不正対策方法：不正注文検知サービス「O-PLUX」について





小野瀬氏は「変化する不正手口を理解したうえで、自社にあった対策を選択していくことが必要である」とお話がありました。

■EC 事業者による取り組みやフィッシング等に関する最新の不正事例■

一般社団法人キャッシュレス推進協議会　福田　好郎氏（事務局長／常務理事）

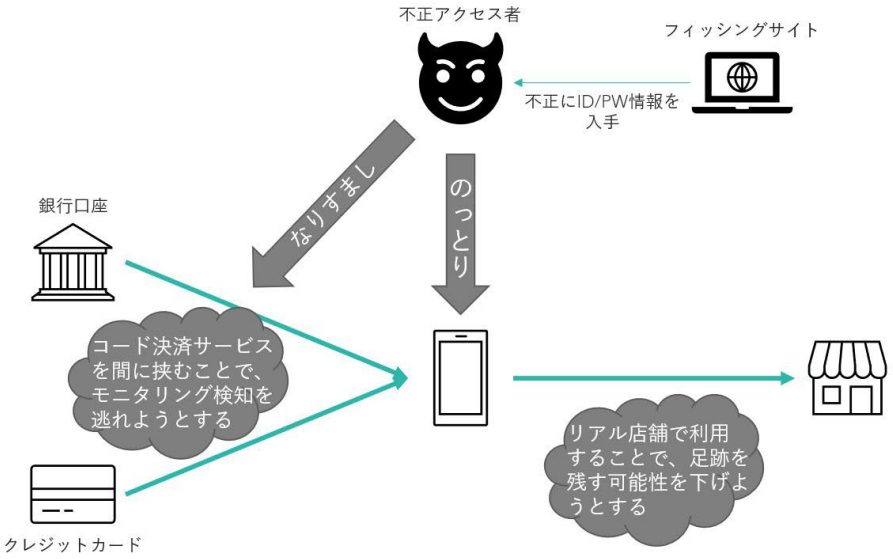
キャッシュレス推進協議会からは「当協議会におけるセキュリティへの取り組み」についてお話をいただきました。

「一般社団法人キャッシュレス推進協議会は、キャッシュレスの普及に向けて活動している。キャッシュレス決済を利用していない方の声として多いのがサービスのセキュリティへの不安がある点が多いことからセキュリティへの対策を重要視している。

コード決済を狙った不正利用は増加している。手口としては、自身のアカウントに他人のクレジットカード情報を紐づける『なりすまし』や、コード決済の ID とパスワードを盗み、アカウントを乗っ取る形がある。コード決済を間にはさむことでモニタリング検知を逃れようとしたり、またリアル店舗で利用することで足跡を残す可能性を下げようとするのなど手口が巧妙化している。

狙われやすいコード決済

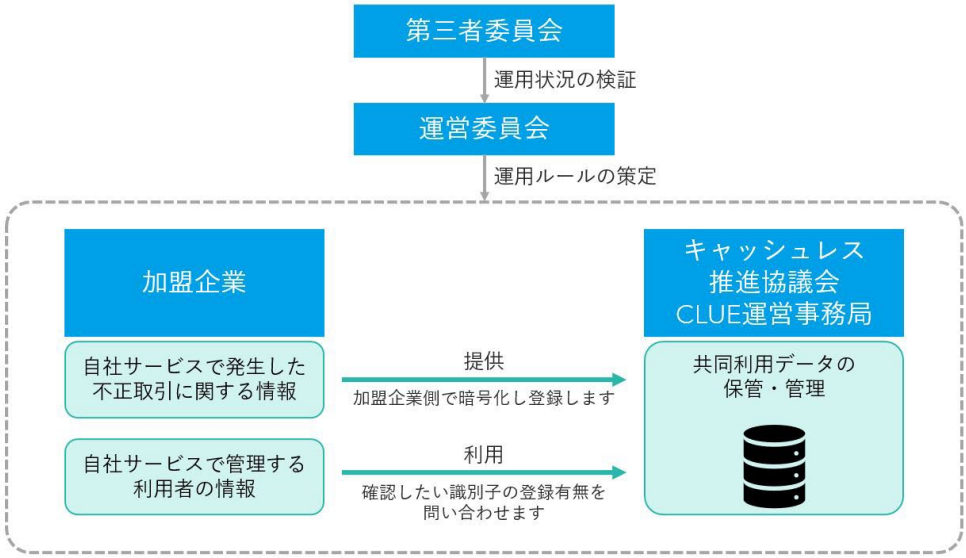
コード決済は、リアル店舗での決済に用いられ、かつ、様々な資金源を紐付けできるという点において、不正利用に狙われやすい。



不正利用に対しては、それぞれの決済事業者が対策進めるが、他の多数の事業者にも同様の不正利用を行うため、個社ごとの情報を共有・連携し業界全体での取り組みが必要とされる。そのため、不正利用情報確認データベース『CLUE』を開発し、被害にあった事業者はその内容をデータベースに登録し、他社間で情報共有、早い段階での不正利用防止を目指しており、この後はコード決済事業者だけでなく、EC 事業者やその他のオンラインサービス事業者にも利用できるよう検討している」とご説明いただきました。

CLUEの概略

不正利用情報確認データベース（CLUE：Cross-referencing List of User Encrypted data）は、不正利用を行った者を特定する識別子（※１）に関する情報を事業者間で共有することにより、同じ識別子を利用する者の取引を調査・警戒等することにより、不正な取引を防止することを目的とします。



福田氏は「不正利用への対策は、事例や対策の情報共有の場を持ち、業界全体あるいは業界の垣根を超えて取り組むべき課題である」とお話がありました。

ヤフー株式会社　コマースインフラ本部安全対策部 部長　藤田 智子氏

ヤフー株式会社からは「ヤフーのコマースサービスにおけるクレジットカード不正利用対策の取り組み」についてお話をいただきました。

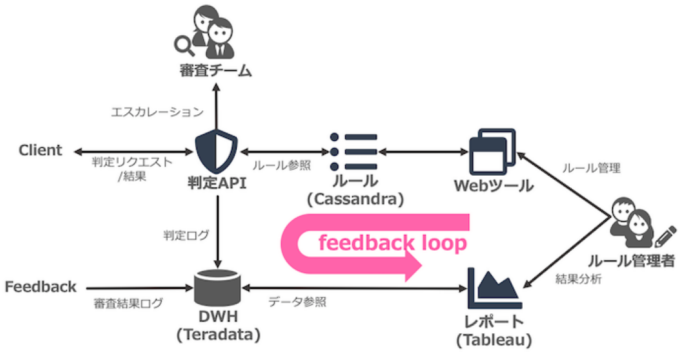
「事業の急激な拡大にともない、ショッピング事業（Yahoo!ショッピング、PayPay モール）、リユース事業（ヤフオク!、PayPay フリマ）の不正利用額が、2019 年にかけて不正利用も増加していたが、不正検知システムの導入の効果から、2020 年以降は抑えられている。カード不正利用に対しては、準備・決済・被害においてさまざまな対策に取り組んでいる。

なかでも特に重要な、決済での対策には、独自に開発した不正検知システムによる判定と人による目視チェックを組み合わせた判定フローを採用している。システムによる判定はルールベースと機械学習を組み合わせ、リアルタイムで判定する。目視チェックは、システムで判断ができない事案について、24 時間 365 日体制で行っている。

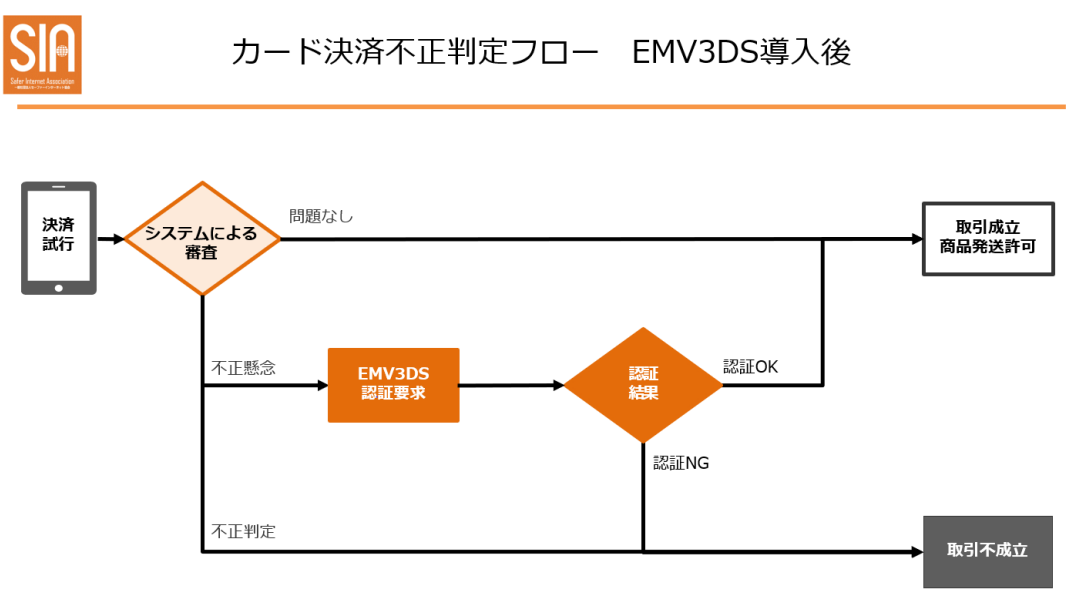
ルールベース判定と機械学習を融合した検知システム

Yahoo! JAPAN Tech Blog

https://techblog.yahoo.co.jp/entry/2021031530118884/



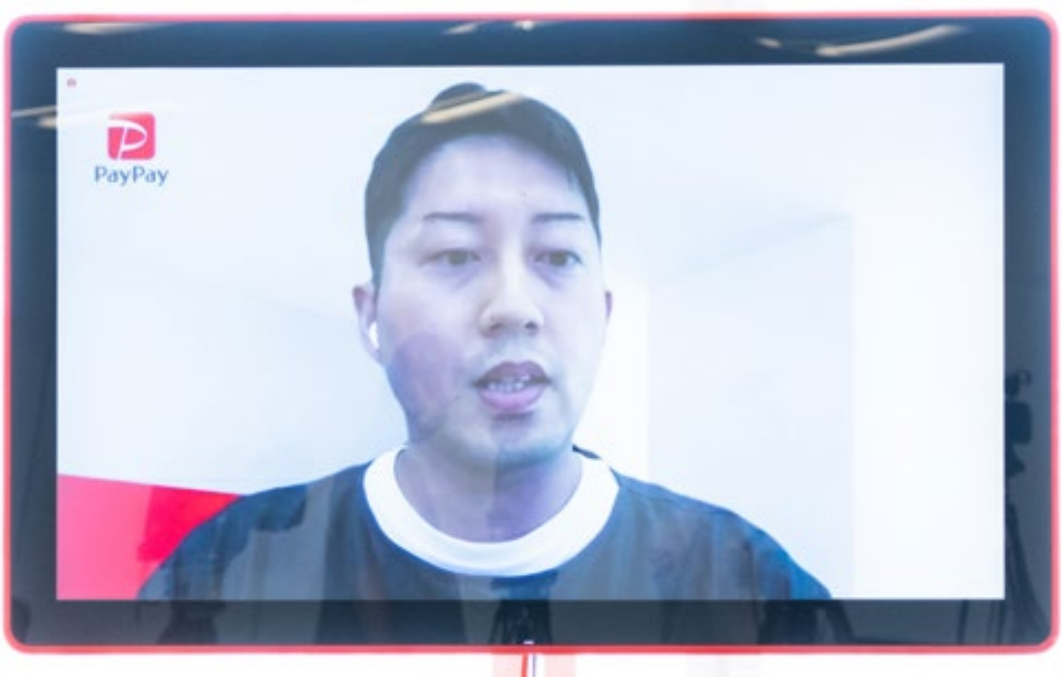
さらに 2022 年 8 月 17 日から、EMV3-D セキュアを導入した。すべての決済情報を EMV3-D セキュアに回すのではなく、目視により行っていた不正懸念のある決済のみを回すことで、業務工数削減が図れ、また、商品の発送が保留されるユーザーを待たせるといった状況も改善できた。



また準備の段階では、ID 悪用対策として新規 ID 取得時に携帯番号を必須することで ID の大量取得がしづらくなるという取り組みが多な我、被害が発生したときの補償制度も導入している。」とご説明いただきました。

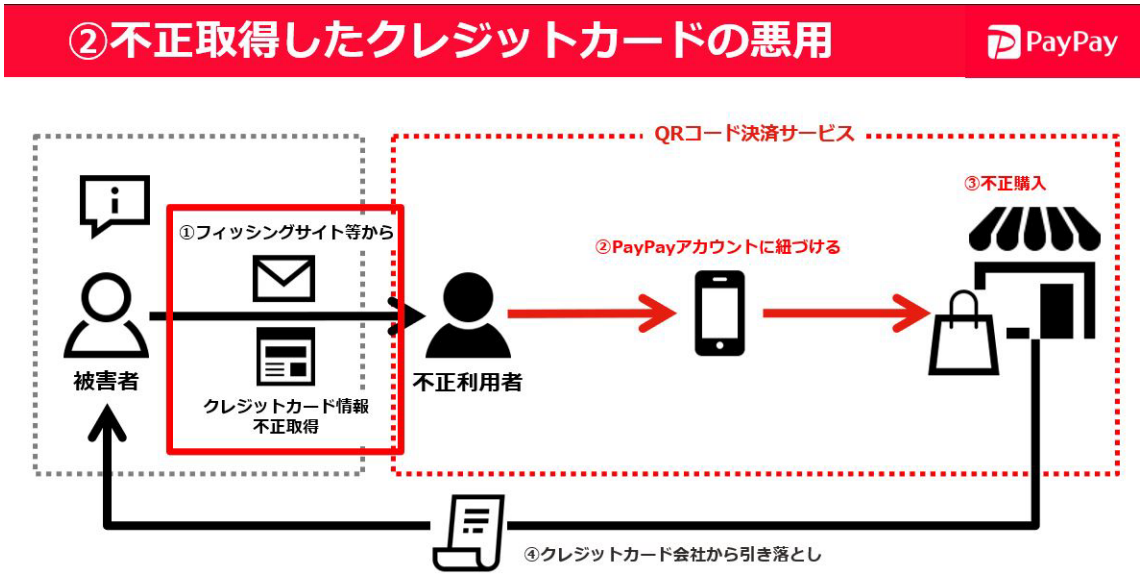
最後に藤田氏は「これらの対策により、不正利用をさせない売場づくり、および検知システムの向上を取り組んでいく」とお話がありました。

PayPay 株式会社　法務リスク管理本部金融犯罪対策室　マネージャー



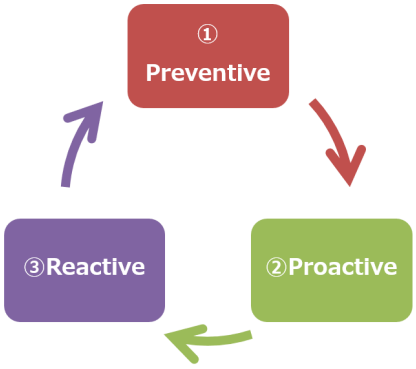
水嶋 康一朗氏
PayPay 株式会社からは「PayPay(コード決済)におけるセキュリティ対策」についてお話をいただきました。

「PayPay のサービスは対面の支払い時に利用されるイメージがあるが、オンラインでも利用されている。PayPay を不正に利用する方法には大きく 2 パターンある。1 つ目はフィッシングによるアカウントの乗っ取りで、不正者がフィッシングで認証情報を盗み、被害者から乗っ取ったアカウントで不正購入を行う。フィッシングには、フィッシングメールの他、偽の SNS 広告からフィッシングサイトに誘導して認証情報を盗むケースも出てきている。2 つ目は不正者がフィッシングサイトからクレジットカードの情報を取得し、自分のアカウントに紐付け、不正購入するパターン。



同社では『事前防止措置』、『積極的な対応』、『ユーザーケアと調査・分析』という 3 つのポリシーにより不正利用の対策を行っている。

3つのリスク対応ポリシー



① Preventive（事前防止措置）

犯罪者のターゲットになりにくいサービス・プロダクト設計

② Proactive（積極的な対応）

不正を早期に検知して利用させない体制

③ Reactive（ユーザーケア・調査／分析）

万一利用されてしまった場合のサポート体制

事案の調査/分析をとおして事前防止方法のリスク対応へ

『事前防止措置』としては、オンライン決済で加盟店のサイトやアプリからPayPay で支払う際は本人確認を漏れなく実施するようになっている。またクレジットカードによる支払の上限金額は、認証状況によりわけており EMV 3-D セキュアや利用実績などを基にした独自基準による上限金額を設けている。

『積極的な対応』では、システムと専門スタッフによる目視（24 時間 365 日体制）により不正を積極的に見つる体制を構築している。

『ユーザーケアと調査・分析』では万が一、不正が発生した場合に対応すべく、24時間体制で電話でのサポートを受け付けている。また被害者や加盟店への補償制度も実施している」とお話をいただきました。

株式会社メルカリ　執行役員 VP of Trust and Safety Japan Region
篠原孝明氏

株式会社メルカリからは「メルカリでの不正利用の実態と対策」についてお話をいただきました。

「メルカリでは 2021 年末から不正利用が増加していたが、対策の強化により、2022 年 7 月以降は大幅に減少傾向にある。
不正利用は、フィッシングとクレジットカードの不正利用の2つがある。最近のメルカリを装うフィッシングサイトは、本物と見分けがつきづらくなっており、利用者には送信元メールアドレスを確認するなどの対応が求められる。

不正利用に対しては、『未然防止』と『早期対策』という 2 軸で対策を推進している。1 つ目の『未然防止』としては、EMV3-D セキュアを導入することで、カゴ落ちを減少させながら、不正利用を防ぐことができ有用である。またフィッシング対策としては、普段利用していない端末からアクセスがあった際の SMS 認証を追加し、送信さる文面には送信理由を明記することで、利用者が第三者の不正利用に気づきやすくしている。

不正利用への対策

メルカリグループでは「未然防止」と「不正検知後の早期対策」の2軸を推進
直近の不正件数は減少傾向にあり一定の成果をあげている

クレジットカード不正利用／不正決済の対策

- **不正利用の未然防止**
  - EMV-3Dセキュアの導入
  - 一部外部店舗での利用制限
- **不正利用への対策**
  - 不正決済・取引検知ルールの定期的な見直し
  - 不正検知後の身分証を用いた本人確認の実施

フィッシングの対策

- **フィッシングの未然防止**
  - お客さまへの注意喚起
  - 公式からのメール案内文等の工夫
  - フィッシングサイトのtakedown
- **不正利用への対策**
  - 追加的なSMS認証（あんしん支払い設定）
  - ログイン時の端末判定　etc

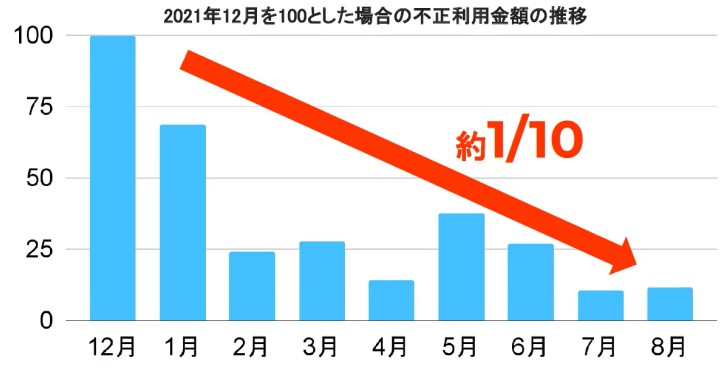
mercari

11

EMV-3D セキュア導入の成果としては、決済の離脱率は 2%前後に抑えられており、カゴ落ちの影響を少なくできている。他方、不正利用の金額は実装前にくらべて 1/10 程度まで減少させることに成功している。

EMV-3Dセキュア導入後の成果

導入前後のお客さまの離脱差分は2～3%前後であり、カゴ落ちの影響は軽微に
一方で、不正利用の金額は導入の効果により2021年12月比で約1/10に減少、
また、EMV-3Dセキュアを逃れるような動き（アプリのダウングレード、開放対象外のカードブランドや経路等）が見られ、対策としての有効性が確認された



mercari

14

今後はアカウント作成時や不正ログインといった、最初の部分についての対策を強化していく」とご説明いただきました。

最後に篠原氏は「事業者と不正者の間でいたちごっこになりつつある。官民が連携し、対策と効果を共有することで、未然に不正利用に対応することが求められる」とお話がありました。